

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A system for distributing cryptographic keys for encrypting digital data, the system comprising:

a source side comprising:

a first memory for storing a cryptographic key[[;]], and

a digital data input medium for receiving digital data to be encrypted;

a display side coupled to the source side via a digital link, comprising a second memory;

a multiplexer coupled to the digital data input medium, the multiplexer multiplexing ~~and for transmitting~~ transmission of the digital data [[or]] and the cryptographic key on the digital data input medium; and

a selector, wherein the selector: [[for]]

couples ~~coupling~~ the first memory to the second memory via the digital data input medium,

receives ~~the selector for receiving~~ the digital data and the cryptographic key from the multiplexer, and

provides ~~for providing~~ the cryptographic key to the second memory,

wherein the second memory is used to store the cryptographic key temporarily on the display side before the cryptographic key is used for encrypting the digital data.

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

2. (Original) The system according to claim 1, wherein the digital data comprises digital video data.

3. (Original) The system according to claim 2, wherein the digital video data is in composite RGB format.

4. (Original) The system according to claim 1, wherein the digital data comprises multimedia data.

5. (Original) The system according to claim 1, wherein the digital data is encrypted in accordance with the High-bandwidth Digital Content Protection specification.

6. (Original) The system according to claim 1, wherein the second memory and the selector are implemented on a single integrated circuit chip.

7. (Currently Amended) A method for distributing an encryption key for encrypting digital data, the method comprising:

selecting an encryption key from a first set of encryption keys stored in a first memory on a source side;

transferring the selected encryption key from the first memory to a second memory on a display side over a digital data transfer medium that is also used for transferring the digital data to be encrypted, using a multiplexer coupled to the digital data transfer medium to ~~transmit~~ multiplex transmission of the digital data [[or]] and the selected encryption key on the digital data transfer medium;

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

receiving the selected encryption key from the multiplexer into a selection switch that provides the selected encryption key to the second memory on the display side; and

storing the selected encryption key temporarily in the second memory on the display side until it is used by an encryptor to encrypt the digital data,

wherein the display side is coupled to the source side via a digital link.

8. (Original) The method according to claim 7, wherein the digital data comprises digital video data.

9. (Original) The method according to claim 8, wherein the digital video data is in composite RGB format.

10. (Original) The method according to claim 8, wherein the digital data comprises multimedia data.

11. (Original) The method according to claim 7, wherein the first set of encryption keys includes keys compatible with the High-bandwidth Digital Content Protection specification.

12. (Currently Amended) A system for encrypting digital data, the system comprising:

a source side comprising:

a first input terminal for receiving the digital data[[]], and

a second input terminal for receiving a key;

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

a multiplexer coupled to the first input terminal and the second input terminal, wherein the multiplexer multiplexes output of the digital data from the first input terminal and the key from the second input terminal;

a display side coupled to the source side via a digital link, comprising a display side memory;

an encryptor for receiving and encrypting the digital data using the key and the display side memory;

a selector switch for receiving the digital data and the key from the multiplexer, wherein the selector switch provides the digital data and the key to the encryptor, the key being temporarily stored in the display side memory; and

a first output terminal for transmitting the encrypted digital data,

wherein the system receives the key from an external key storage medium via the second input terminal ~~during operation of the system.~~

13. (Currently Amended) The system for encrypting digital data according to claim 12, wherein the display side memory is a ~~the system further comprising~~ random access memory (RAM) ~~for storing the key before the key provided to the encryptor to be used for encryption of the digital data.~~

14. Cancelled.

15. Cancelled.

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

16. (Original) The system for encrypting digital data according to claim 12, wherein the key includes an encryption key, which is used for encrypting the digital data.

17. (Original) The system for encrypting digital data according to claim 12, wherein the second input terminal receives the key as a plurality of key segments.

18. (Original) The system for encrypting digital data according to claim 12, wherein the key includes a decryption key, which is used for decrypting the encrypted digital data.

19. (Original) The system for encrypting digital data according to claim 18, wherein the first output terminal is used to transmit the decryption key.

20. (Original) The system for encrypting digital data according to claim 19, wherein the decryption key is encoded prior to being transmitted via the first output terminal.

21. (Original) The system for encrypting digital data according to claim 20, wherein the key includes an encoding key, and the encoding key is used to encode the decryption key in the encryptor before the decryption key is transmitted via the first output terminal.

22. (Original) The system for encrypting digital data according to claim 12, wherein the digital data comprises digital video data.

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

23. (Original) The system for encrypting digital data according to claim 22, wherein the digital video data is in composite RGB format.

24. (Original) The system for encrypting digital data according to claim 12, wherein the digital data comprises multimedia data.

25. (Original) The system for encrypting digital data according to claim 12, wherein the encryptor complies with the requirements of the High-bandwidth Digital Content Protection (HDCP) specification.

26. (Original) The system for encrypting digital data according to claim 12, wherein the first input terminal, the second input terminal, the encryptor and the first output terminal are implemented on a single integrated circuit (IC) chip.

27. (Original) The system for encrypting digital data according to claim 12, wherein the second input terminal comprises a control bus, and wherein the system further comprises a controller coupled to the control bus, wherein the controller controls data flow in the system.

28. (Original) The system of encrypting digital data according to claim 27, wherein the control bus comprises an I²C bus.

29. (Original) The system of encrypting digital data according to claim 27, wherein the controller is selected from a

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

group consisting of a finite state machine (FSM), a microprocessor and a micro controller.

30. (Currently Amended) A method of encrypting digital data in a data encryption system, the method comprising the steps of:

receiving the digital data;

receiving a key from an external key storage medium at a source side of the data encryption system;

encrypting the digital data using the key, the key being temporarily stored at a display side memory of a display side of the data encryption system; and

transmitting the encrypted digital data as an output, wherein the display side is coupled to the source side via a digital link.

~~wherein the steps of receiving the digital data and receiving the key are performed during operation of the data encryption system.~~

31. (Currently Amended) The method according to claim 30, wherein the display side memory is a ~~the method further comprising the step of storing the key in random access memory (RAM) before the key is used for encryption of the digital data.~~

32. (Original) The method according to claim 30, wherein the key includes an encryption key, and the encryption key is used for encrypting the digital data.

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

33. (Original) The method according to claim 30, wherein the step of receiving the key comprises the step of receiving a plurality of key segments.

34. (Original) The method according to claim 30, wherein the key includes a decryption key, and the decryption key is used for decrypting the encrypted digital data.

35. (Original) The method according to claim 34, the method further comprising the step of transmitting the decryption key.

36. (Original) The method according to claim 35, the method further comprising the step of encoding the decryption key before it is transmitted.

37. (Original) The method according to claim 36, wherein the key includes an encoding key, and the encoding key is used to encode the decryption key before the decryption key is transmitted as the output.

38. (Original) The method according to claim 30, wherein the digital data comprises digital video data.

39. (Original) The method according to claim 38, wherein the digital video data is in composite RGB format.

40. (Original) The method according to claim 30, wherein the digital data comprises multimedia data.

41. (Original) The method according to claim 30, wherein the step of encrypting the digital data complies with

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

the requirements of the High-bandwidth Digital Content Protection (HDCP) specification.

42. (Previously Presented) A system for distributing cryptographic keys from a digital data transmitter to a digital data receiver via a digital link, the system comprising:

a digital data transmitter comprising:

a first key storage medium for storing a first encryption key, a second encryption key and a first decryption key, which is different than the first encryption key;

a data encryptor having a first port and a second port, the data encryptor for using the first encryption key to encrypt digital data, and for using the second encryption key to encrypt the first decryption key;

a multiplexer coupled to the first key storage medium, wherein the multiplexer outputs digital data or at least one of the first encryption key, the second encryption key and the first decryption key from the first key storage medium;

a selector switch for receiving the digital data and the at least one of the first encryption key, the second encryption key and the first decryption key from the multiplexer, wherein the selector switch provides the digital data to the encryptor via the first port, and wherein the selector switch provides the at least one of the first encryption key, the second encryption key and the first decryption key to the encryptor via the second port; and

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

a data link transmitter system for transmitting the encrypted digital data and the encrypted first decryption key over the digital link; and

a digital data receiver comprising:

a data link receiver for receiving the encrypted digital data and the encrypted first decryption key over the digital link;

a second key storage medium for storing a second decryption key;

a data decryptor for using the second decryption key to decrypt the encrypted first decryption key, and for using the first decryption key to decrypt the encrypted digital data; and

a third key storage medium for storing the first decryption key.

43. (Original) The system according to claim 42, wherein the digital data transmitter comprises a Digital Versatile Disk (DVD) player.

44. (Original) The system according to claim 42, wherein the digital data comprises digital video data.

45. (Original) The system according to claim 42, wherein the digital data comprises multimedia data.

46. (Original) The system according to claim 42, wherein the second encryption key comprises a public key and the second decryption key comprises a private key.

1

Appln No. 09/844,898

Amdt date February 21, 2006

Reply to Office action of December 14, 2005

47. Cancelled.

48. (New) The system for encrypting digital data according to claim 12, wherein the display side memory is an integral component of the encryptor.